MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2016/2017

TSN3251 / TSC2211 – COMPUTER SECURITY

(All Sections / Groups)

7 October 2016
9:00 a.m. – 11:00 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This paper consists of 7 pages (including cover page) with 5 Questions only.
2. Attempt **ALL FIVE** questions. The distribution of the marks for each question is given. This paper carries **100 marks**.
3. Please print all your answers in the Answer Booklet provided.

Question 1 (20 Marks)

a) Explain the following principles in computer security.

i. Principle of Adequate Protection
ii. Principle of Easiest Penetration
iii. Principle of Effectiveness

[3 marks]

b) Confidentiality, integrity and availability (CIA), is a model designed to guide policies for information security within an organization. In your own words, explain and give an example each on what is meant by the THREE (3) terms: **confidentiality**, **integrity** and **availability**.

[6 marks]

c) Differentiate between Steganography and Cryptography.

[1 mark]

d) If plaintext is denoted by P, ciphertext is denoted by C, the encryption function is denoted by E( ) and the encryption key is denoted by K_s, write down the formal notation relating plaintext and ciphertext.

[2 marks]

e) A computer security threat is blocked by the controls you put in place on your system's vulnerability. The controls that are put into place are the defence mechanisms and the simplest mechanism is to prevent access to the vulnerability. State and give a brief description of the other FOUR (4) defence mechanisms.

[4 marks]

f) Encrypt the following sentence with key substitution cipher using the key "MULTIMEDIA".

"top university"

In your answer, copy the following table to show how you did your encryption.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

[4 marks]

Continued ...

Question 2 (20 Marks)

a) Decrypt the following message that was encrypted using the Playfair cipher with the key "people". Ensure that you show each step you did to decrypt it clearly.

GUCSEKFKONCW

[6 marks]

b) Given the following 2 by 2 matrix, $\begin{bmatrix} 4 & 5 \\ 3 & 1 \end{bmatrix}$, compute the inverse of the matrix in modulo 26 arithmetic. You are also required to show that you have derived the inverse correctly.

$$\begin{bmatrix} 4 & 5 \\ 3 & 1 \end{bmatrix}^{-1}$$

[8 marks]

c) Encrypt the following plaintext using a 5-row railfence cipher (ignore the spaces).

fencing is a sport

[3 marks]

d) Explain why the Frequency Distribution method is not effective on ciphertext that has been encrypted using the transposition method.

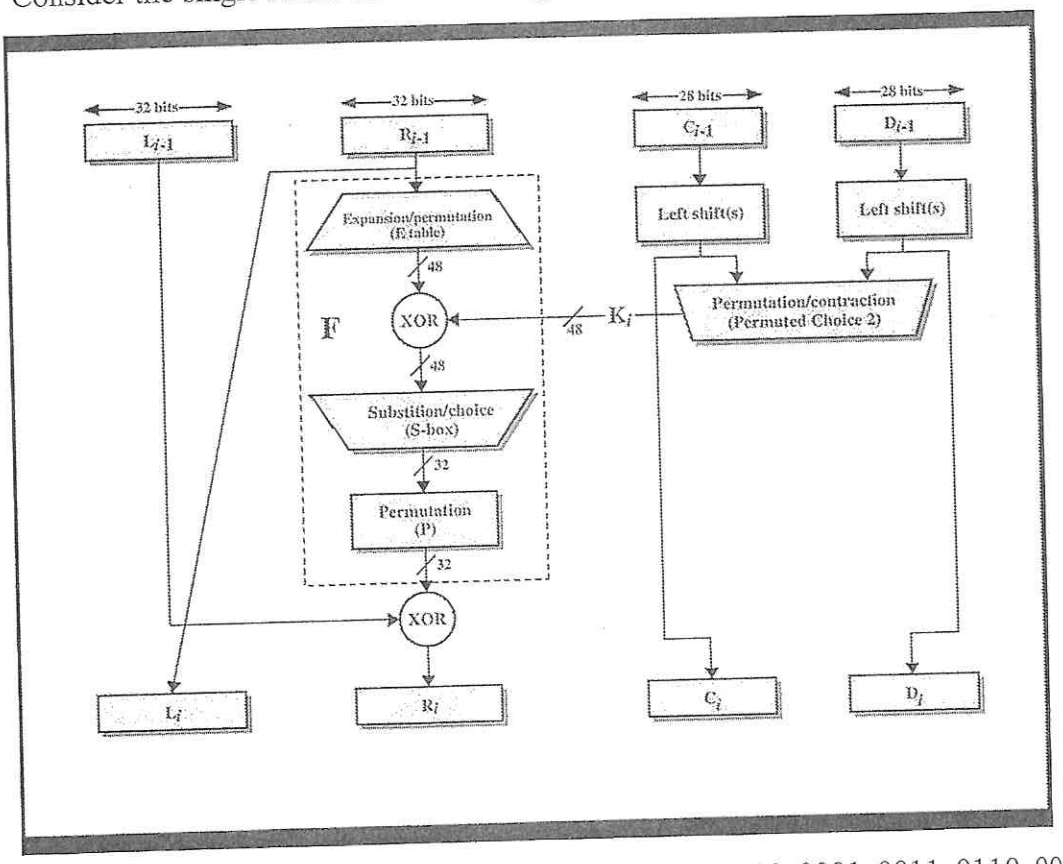
[2 marks]

e) State the goal of encryption by transposition as opposed to the substitution method.

[1 mark]

Question 3 (20 Marks)

a) Consider the single round of the DES Algorithm as depicted in the figure below.



For the sixth round, given that L_5 is "0000 1010 1010 0001 0011 0110 0010 1111" and R_5 is "1101 1101 0000 0011 0101 1101 1110 1101". Use the *E Table* to compute the output after the Expansion/Permutation stage.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Expansion/Permutation (E)

[5 marks]

Continued ...

b) Euler's Theorem is a generalization of the Fermat's theorem. It is stated as

$$a^{\phi(n)} \bmod n = 1, \text{ where } \gcd(a,n)=1$$

Show how you can solve $7^{503} \bmod 13$ using the Euler's Theorem (hint: you can use the square and multiply rule).

[8 marks]

c) RSA is the best known and most widely used algorithm for Public Key Cryptography. State the steps for RSA Key Generation.

[4 marks]

d) Explain the steps for Birthday Attacks on Hash Functions.

[3 marks]

Question 4 (20 Marks)

a) Programmers do make errors that can cause program malfunctions and a few classes of errors have plagued programmers and security professionals for decades. Three (3) classic error types that have enabled many security breaches are (i) Buffer Overflows, (ii) Incomplete Mediation, and (iii) Time-of-Check to Time-of-Use Errors. Explain each of the three (3) types mentioned above and also state how they can be prevented or mitigated.

[6 marks]

b) Give an overview of Database SQL Injection attack and explain technically how it works. (You may use code snippet to explain if needed).

[4 marks]

Continued ...

c) In the Linux Operating System, the users' passwords are stored in the file `/etc/shadow`. An example of a line from the file is as follows:

```
niantic:$6$3WWbKfr1$4vblknvGr6FcDeF92R5xF/n:15045:0:99999:7:::
```

Identify which is the user login identity, the encrypted password, the salt and the hash encryption algorithm indicator.

[4 marks]

d) Explain what is a cryptography salt. How can it be used to defend against dictionary attacks?

[2 marks]

e) Memory protection in an operating system is one of the most elementary requirements in a multi-program system. With the aid of diagrams, explain the following techniques that can be used to provide protection between the operating system's memory space and the user program's memory space.

i. Fence Register

ii. Bound Registers

[4 marks]

Continued ...

Question 5 (20 Marks)

a) There are many concerns (issues) for security in a network. One of them is because of "sharing". In sharing the resource and workload of networks, more users have the potential to access networked systems than single computers. State and explain at least another THREE (3) issues of network security?

[6 marks]

b) In network security threats, explain the following terms.

i. Inductance in wiretapping attacks

ii. Phishing in Man-in-the-Middle attacks

[2 marks]

c) State and discuss any TWO (2) advantages and TWO (2) disadvantages of using biometrics as a method of authentication.

[4 marks]

d) There are many types of Denial of Service (DOS) attacks. One of them is called SYN-Flooding. Give a detailed explanation on how SYN-Flooding achieves a DOS. Detailed description needed.

[3 marks]

e) Briefly describe any 5 (FIVE) (out of the 7) issues that are addressed by a security plan.

[5 marks]

END OF EXAM PAPER